

AFFIDAVIT IN SUPPORT OF COMPLAINT AND ARREST WARRANT

I, Kelly M. Bell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent for the Federal Bureau of Investigation (“FBI”) for more than 18 years. I am currently assigned to the FBI’s Boston Field Office, where I investigate wire fraud, bank fraud, money laundering, bankruptcy fraud, and mortgage fraud, among other economic crimes. I have received on-the-job and FBI-sponsored training concerning these types of investigations, and my experience includes the execution of search, seizure, and arrest warrants.

2. I submit this affidavit in support of an application for a criminal complaint charging Hui Zhang (“Zhang”) with bank fraud, in violation of 18 U.S.C. § 1344, and for a warrant for his arrest. As set forth below, I have probable cause to believe that, from in or around June 2020 through at least May 2022, Zhang executed a scheme to defraud First Republic Bank and to obtain money under the custody and control of First Republic Bank. This scheme involved the opening of bank accounts under false identities (the “Fraudulent Bank Accounts”), the depositing of counterfeit First Republic Bank checks into the Fraudulent Bank Accounts, and the withdrawal of funds derived from the depositing of the counterfeit checks from the Fraudulent Bank Accounts.

3. Specifically, this scheme involved 114 counterfeit checks totaling \$1,035,350 being deposited into the Fraudulent Bank Accounts, and a man subsequently identified as Zhang withdrew hundreds of thousands of dollars in cash from these accounts via ATM. Zhang was identified in part by a tattoo on his left hand that was depicted in certain ATM surveillance

videos. In addition, Zhang has been tied to an IP address that was used to open one of the Fraudulent Bank Accounts, and to deposit counterfeit checks into that account.

4. The facts in this affidavit come from my participation in this investigation, including my personal observations and review of records, my training and experience, and information obtained from other law enforcement personnel and witnesses. In submitting this affidavit, I have not included every fact known to me about this investigation. Rather, I have included only those facts that I believe are sufficient to establish probable cause for a criminal complaint charging Zhang with bank fraud, in violation of 18 U.S.C. § 1344.

PROBABLE CAUSE

At all times relevant to this affidavit:

5. Zhang, age 41, was a resident of Quincy, Massachusetts.
6. “Victim Company” was a family business located in Boston, Massachusetts.
7. “Individual 1” was a resident of Quincy, Massachusetts.
8. “Individual 2” was a resident of Boston, Massachusetts.

Overview of the Fraud Scheme

9. In or about May 2022, the owners of the Victim Company discovered a counterfeit check scheme affecting their business. Between June 2020 and May 2022, at least 114 counterfeit checks totaling \$1,035,350 were drawn against the Victim Company’s account at First Republic Bank.¹

¹ At the relevant times, the deposits of First Republic Bank were insured by the Federal Deposit Insurance Corporation (FDIC). According to the FDIC’s website, First Republic Bank was insured by the FDIC until the bank closed on May 1, 2023.

10. From May 2022 to July 2022, several additional counterfeit checks posted to the Victim Company's account, but First Republic Bank declined to process them due to fraud.

11. First Republic Bank only reimbursed the Victim Company for \$48,150 in damages. Therefore, the total loss to the Victim Company is \$987,200.

12. Before the scheme was discovered, 61 counterfeit checks totaling \$569,730 were deposited into PNC Bank account number x-6653 (the "PNC Bank account"). All of these checks were deposited electronically using PNC Bank's mobile check deposit application.

13. In addition, 45 counterfeit checks totaling \$398,900 were deposited into Ally Bank checking account number x-4333 (the "Ally Bank checking account"), and three counterfeit checks totaling \$23,800 were deposited into Ally Bank savings account number x-9847 (the "Ally Bank savings account"). All of these checks were deposited electronically using Ally Bank's eCheck mobile deposit system.

The PNC Bank Account

14. On or about June 5, 2020, the PNC Bank account was opened online in the name of Individual 1, using his name, date of birth, and Social Security number.

15. The Internet Protocol (IP) address used to open the PNC Bank account was 24.91.184.31. From August 2020 to August 2021, this same IP address was used to deposit nine counterfeit checks.

16. According to publicly available information, IP address 24.91.184.31 is assigned to Comcast and geo-located in Quincy, Massachusetts. Due to Comcast's retention policy, by the time of this investigation, subscriber records for the relevant time period were no longer available.

17. According to PNC Bank records, for the period November 2020 to May 2022, 44

counterfeit checks were deposited into the PNC Bank account using various IP addresses assigned to T-Mobile. At least 15 of the counterfeit checks were deposited using an iPhone.

18. From April 2021 to January 2022, PNC Bank's mobile banking application captured GPS coordinates for the device(s) used to deposit 26 of the counterfeit checks. Of these, 24 checks were deposited at or very close to 437 Willard Street, Quincy, Massachusetts. The other two checks were deposited in Edmond, Oklahoma, a city located within the Oklahoma City metropolitan area.

19. In addition to the \$569,730 in counterfeit checks deposited directly into the PNC Bank account, \$8,500 was transferred from the Ally Bank checking account to the PNC Bank account. Apart from these two sources, only a few hundred dollars were deposited into the PNC Bank account.

20. For the period June 5, 2020 to June 16, 2022, when the PNC Bank account was closed, there were at least 699 withdrawals at automated teller machines (ATMs). These withdrawals totaled over \$440,000 in cash.

21. For example, on or about May 17, 2022, a counterfeit check that purported to be written on the Victim Company's account with First Republic Bank (account ending 1669, check number 37661) was mobile deposited into the PNC Bank account.

The Ally Bank Checking Account

22. On or about March 31, 2020, the Ally Bank checking account was opened online in the name of Individual 2, using his name, date of birth, and Social Security number.

23. A telephone number associated with the Ally Bank checking account was the same as a telephone number associated with the PNC Bank account.

24. Besides the \$398,900 in counterfeit checks, only \$2,100 was deposited into the

Ally Bank checking account from other sources. In addition, \$20,850 was transferred from the Ally Bank savings account into the Ally Bank checking account.

25. For the period March 31, 2020 to May 18, 2022, when the Ally Bank checking account was closed, over \$350,000 was transferred to other bank accounts, including the PNC Bank account and other accounts opened in the name of Individual 2.

The Ally Bank Savings Account

26. On or about July 10, 2020, the Ally Bank savings account was opened online in the name of Individual 2, using his name, date of birth, and Social Security number.

27. The only deposits into the Ally Bank savings account were three counterfeit checks totaling \$23,800 and a transfer of \$2,800 from the Ally Bank checking account. Of the total amount deposited into the Ally Bank savings account, almost all of the funds were transferred to the Ally Bank checking account, as mentioned above.

ATM Withdrawals of Stolen Funds

28. I have reviewed surveillance videos and photographs of ATM withdrawals from the PNC Bank account that were made at several other banks in 2021 and 2022.

29. From October 3, 2021 through December 22, 2021, there were 16 ATM withdrawals totaling \$8,056 made at the following three Massachusetts Rockland Trust locations: the Kneeland Street Branch, 95 Kneeland Street, Boston; the Andrew Square Branch, 501 Southamptton Street, South Boston; and the North Quincy Branch, 495 Hancock Street, Quincy.

30. I have reviewed surveillance photographs for several withdrawals made at the Kneeland Street Branch and the Andrew Square Branch, and these images all appear to depict the same individual. On three different dates, this person wore the same gray jacket that has red

sleeves and a red triangle surrounding a drawing of an eye on the left breast.² Below is a surveillance photo of an ATM withdrawal on October 3, 2021 at the Kneeland Street Branch:



31. Likewise, below is a surveillance photo of an ATM withdrawal on October 14, 2021 at the Andrews Square Branch:



In an October 15, 2021 surveillance photo (below) from the Kneeland Street Branch, the same person appears to be holding a cell phone while withdrawing funds from the ATM.

² A search of publicly available information revealed that this designer bomber jacket was made by Gucci and sold for approximately \$3,950.



32. I have also reviewed surveillance photographs for withdrawals from the PNC Bank account that were made at Citizens Bank. From December 26, 2021 through April 23, 2022, there were 30 ATM withdrawals totaling \$15,105 made at two Citizens Bank locations: 580 Washington Street, Boston and 50 Summer Street, Boston.

33. Surveillance photographs for several withdrawals from the Washington Street location appear to depict the same person described above. On two different dates, this individual wore the same gray jacket with red sleeves and a red triangle on the left breast. For example, below is a surveillance photo of an ATM withdrawal on April 3, 2022 at the Citizens Bank ATM on Washington Street:



Date: 04/03/2022 23:11:04.73
Camera: 2 MZ3819
Event: Surveillance
DVR: CFG-MA-799-Chinatown

34. On three other dates, Citizens Bank surveillance photos show a similar-looking

person wearing a white jacket with dark skulls drawn on the body and sleeves.³ For example, below is a surveillance photo of an ATM withdrawal on April 7, 2022 at the Citizens Bank ATM on Washington Street:



Date: 04/07/2022 21:20:40.81
 Camera: 2 MZ3819
 Event: Surveillance
 DVR: CFG-MA-799-Chinatown

35. I have also reviewed surveillance videos and photographs for several ATM withdrawals from the PNC Bank account that were made at TD Bank, 323 Hancock Street, Quincy, Massachusetts. From March 12, 2022 through April 27, 2022, there were 10 ATM withdrawals totaling \$9,035 made at this location, and the images appear to depict the same individual, as described above.

36. On two different dates, this person wore the same gray jacket with red sleeves and a red triangle on the left breast. For example, below is a still photo from surveillance video of an ATM withdrawal on March 21, 2022 at the TD Bank branch on Hancock Street:

³ A search of publicly available information revealed that this designer bomber jacket was made by Alexander McQueen and sold for approximately \$2,450.



37. On March 28, 2022, what appears to be the same person made an ATM withdrawal at the TD Bank on Hancock Street while wearing the white jacket with skulls on it. Below is a still photo from the surveillance video of this transaction:



38. While reviewing the TD Bank surveillance videos from March 21, 2022 and March 28, 2022, I observed that the person who made these ATM withdrawals had a tattoo on their left hand between the thumb and index finger, as shown in the close-ups below:



Identification of Hui Zhang

39. According to Melrose Bank records, Zhang became a customer of the bank in August 2019. Zhang used his true name, date of birth, and Social Security number to open multiple bank accounts.

40. From May 2020 to September 2020, Zhang's profile at Melrose Bank was accessed more than 70 times from an iPhone using IP address 24.91.184.31—the same IP address that was used to open the PNC Bank account that received more than \$500,000 in counterfeit checks drawn on the Victim Company. Several checks were deposited remotely into Zhang's own accounts using the same IP address. During the same time period, Zhang's Melrose Bank account was also accessed numerous times using IP addresses assigned to T-Mobile—the provider associated with 44 counterfeit check deposits into the PNC Bank account.

41. According to Cambridge Savings Bank records, Zhang became a customer of the that bank in July 2020. He used his true name, date of birth, and Social Security number to open multiple accounts there. Zhang provided telephone number 781-xxx-0539 for voice calls and text messages.

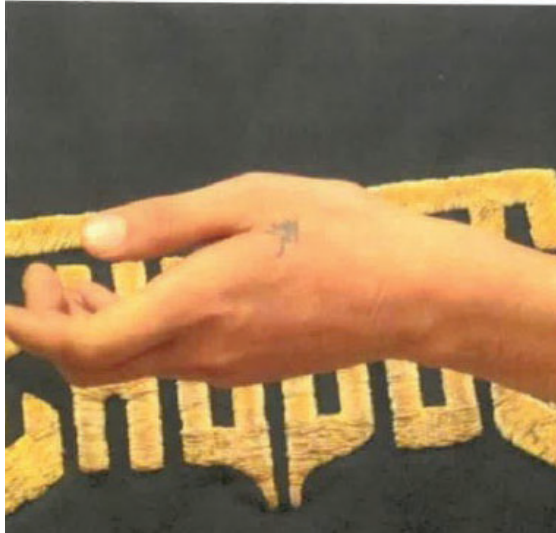
42. From July 2020 to January 2021, Zhang's profile at Cambridge Savings Bank was accessed more than 110 times from an iPhone using IP address 24.91.184.31, and several checks were deposited remotely into Zhang's accounts using the same IP address. During the same time period, this bank account was also accessed numerous times using IP addresses assigned to T-Mobile.

43. On February 7, 2020, Zhang was arrested by the Quincy Police Department for operating a motor vehicle after license suspension. At the time of his arrest, Quincy Police took photographs of Zhang. As demonstrated by the images below, the person in these photos appears

the same or similar to the person depicted in the ATM surveillance footage:



44. Quincy Police also took photographs of Zhang's tattoos, including a tattoo on his left hand. As shown in the close-up photo below, this tattoo appears to match the tattoo on the left hand of the individual depicted in the ATM surveillance footage:



45. Employees of the Victim Company reviewed their records and found that Zhang sold a luxury item to the Victim Company on July 22, 2019. As payment for the luxury item, the Victim Company wrote Zhang a check for \$6,900.

46. The routing number and account number on this legitimate check matched the routing number and account number later printed on the counterfeit checks that were deposited into the accounts referenced above.

47. On July 23, 2019, Zhang deposited the Victim Company's check into a TD Bank account belonging to his spouse. In December 2019, Zhang was added to this account as an authorized signer, and he provided his telephone number as 781-xxx-0539. Between June 2020 and May 2021, IP address 24.91.184.31 was used to access this account four times.

48. I have reviewed telephone records for the mobile phone assigned call number 781-xxx-0539. The service provider for this phone is T-Mobile USA Inc. For the period September 2018 to May 2023, Zhang was the subscriber.

49. I have reviewed casino records and bank records showing that Zhang frequents several casinos located within the Oklahoma City metropolitan area. These include Remington Park in Oklahoma City, Newcastle Casino in Newcastle, and Riverwind Casino in Norman.

CONCLUSION

50. Based on the foregoing, I have probable cause to believe that, on or around May 17, 2022, Hui Zhang knowingly executed, and attempted to execute, a scheme and artifice to defraud a financial institution, that is, First Republic Bank, and to obtain moneys, funds, credits, assets, securities and other property owned by and under the custody and control of First Republic Bank, by means of materially false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.


Respectfully submitted,


Special Agent Kelly M. Bell
Federal Bureau of Investigation

Sworn to by telephone in accordance with Fed. R. Crim. P. 4.1.

11:05 a.m.

Dated: September 6, 2023


Honorable David H. Chase
United States Magistrate Judge

